REMARKS

Claims 1-21 are presented for further examination. Claims 1, 10, 13, 16, and 19 have been amended.

This amendment is supplemental to the Amendment filed on April 2, 2008, with the exception of the deletion of the added phrase "that include picture and sound components" in the preamble of independent claims 1, 10, and 13. In all other respects this Supplemental Amendment is identical to the prior Amendment.

In the final Office Action dated October 3, 2007, the Examiner rejected claims 1-21 under 35 U.S.C. § 103(a) as obvious over previously cited patents to Horne in view of Ishibashi et al. and Yokoyama et al. In remarks accompanying the rejection the Examiner states that applicants' prior arguments against the references individually cannot show nonobviousness, and that recitations in the preamble are not given patentable weight.

Applicants respectfully disagree with the bases for the rejection and request reconsideration and further examination of the claims.

The present disclosure is directed to a method of broadcasting data to customers in a manner that ensures security so that only customers with the correct subscriptions have access to specific data. This is achieved by encrypting control words according to a common key and broadcasting these control words. The common keys are encrypted according to a secret key with the secret key being given to a specific customer's receiving device.

The disclosed embodiments provide for more than one common key to be given to each customer by including a common key store. This permits different common keys to be assigned to different sets of data (such as a different television program), thus providing greater flexibility and control whilst still allowing the common keys to be changed regularly for security purposes.

The difficulty arises when using a common key store because it is possible to read the stored data and determine the common keys. The disclosed embodiments as recited in the claims prevent this possibility of discovering the common keys because the only connection between the common key table and the decryption unit is via a hardware internal bus. Furthermore, even if a malicious party were able to discover the common keys, they would not be able to decrypt the program information because the only way of providing the common key to the decryption unit is by firstly providing the encrypted common key to the decryption unit itself. Without knowing the unit specific secret key, the foregoing would not be possible. If a unit's secret key becomes known, then only the security of that unit is compromised.

Horne, U.S. Patent No. 4,887,296, can only deal with common keys broadcast in real time and, as the Examiner has acknowledged, does not disclose a common key store and has no storage means.

The Examiner argues that it would be obvious to combine the teachings of Horne and Ishibashi et al. (U.S. Patent No. 6,728,379) to arrive at a circuit with a common key store. The apparent motivation to do this is to "transfer data from service providers over an unsecured environment that requires both low processing overhead, yet still prevents an unauthorized user from accessing the data."

Applicants have addressed this in their previous response, which is that the combining of the teachings of Ishibashi and Horne would not lead to a common key store as set forth in the claims and as intended in the current described embodiments.

As mentioned at column 6, lines 25-28, of Ishibashi et al., the "content decryption key" is stored in encrypted form. This is not the current case in the present claimed embodiments whereby the common key must be decrypted using a secret key before it is stored. If the current claimed embodiments allowed the common key to be stored in encrypted form, then it would not be the case that "the only route to placing a common key in the common key store is to put the common key in encrypted form for decryption in accordance with the secret key." Storing in encrypted form would mean that the encrypted common key would need to be input into the store via a route other than through the decryption unit. Such an alternative access route reduces the security of the device and negates the entire point of the present disclosure.

Ishibashi discloses the use of a hard disk drive. A combination of Ishibashi and Horne would merely describe to the skilled person the incorporation of a key store on a separate hard disk and not a key store integrated onto a monolithic device and accessible only over an internal bus by a decryption unit. The difference in security provided by the former arrangement simply does not compare to the latter.

If one of ordinary skill in this art were to combine the key store of Ishibashi et al. with Horne, then, at best, they would produce a device with a memory that stores encrypted keys and is therefore accessible by a route other than by decrypting with a secret key. Notably, the memory would be an external hard drive. This is very different from the current claimed embodiments.

A second point is that combining Horne and Ishibashi et al. as suggested by the Examiner appears to be an application in hindsight. That is, there is simply no motivation to incorporate a key store into Horne. The fact is, the key store incorporated in the claimed embodiments provides different levels of service to individual customers. The present embodiments as set forth in the claims deal with all portions of the broadcast data, and different service levels can be provided on a per-program basis. In contrast, Horne only deals with the audio portion of a broadcast. This stems from the fact that Horne deals essentially with analog broadcasts whereby the audio is separated from the video signal and overlaid at a later point by using a synchronization signal. There would be no point in providing customers with different levels of service for receiving audio unless the same could be achieved with video. Horne is completely silent on the point of providing different service levels to customers, and therefore one of ordinary skill would not be motivated to incorporate a common key store.

An additional point to note is that neither Horne nor Ishibashi, taken alone or in any combination thereof, describe using control words. These are control signals that are broadcast alongside the program data to tell the main processor how to reconstruct the data. The Examiner relies upon a third reference to provide this feature. However, control words are not mentioned in Horne because they are not necessary when dealing only with audio data. There is no teaching or suggestion or motivation to include control words into a device such as that described in Horne. And there is no teaching of control words in Ishibashi et al. because this reference is concerned with network communication and not broadcasts.

The description of control signals mentioned in Yokoyama (U.S. Patent No. 6,625,147) is not equivalent to the "control words" of the present claimed embodiments, which are directed to broadcasts. Yokoyama, in contrast, is directed to communications over a network. Network and broadcast communications are fundamentally different systems, and there is no motivation for one of skill in the area of broadcasts to utilize technology from the area of network security. Yokoyama describes a network control system and is not a customer receiver device. The encrypted control signals of Yokoyama are sent between a network control device and a packet transfer device, which themselves make up the network control system. In other words, the only communication of encrypted control signals is between two components, and in fact this communication is via a cable (see, for example, Figure 3). This cannot be considered broadcasting and is simply not relevant to the current claimed embodiments where control words are broadcasted in encrypted form to many users.

The Examiner suggests that the reasoning for relying upon the teaching of Yokoyama is to "minimize the necessity for storing and protecting a secret key for each receiver in the transmitting site." As discussed above, Yokoyama does not deal with transmitters and receivers in a broadcasting sense, and such an arrangement in isolation (with using secret keys as does the current claimed embodiments) would only have been useful in devices communicating by cable. Using only a common key to broadcast to anyone who can receive the signal with the correct equipment would lead to unique security considerations that are not required or contemplated by Yokoyama.

With respect to the tertiary documents cited by the Examiner, Heer (U.S. Patent No. 5,999,629) and Maari (U.S. Patent Publication No. 2004/0107167) are relied upon as disclosing integrated circuits that have key stores and a processor, along with the encoding/decoding unit in the case of Maari. Applicants respectfully note from Maari that the common-key storage memory (numeral 22 in Figure 2) does not have only one access route for storing the common-key, as required by claim 1. This appears to teach away from the present disclosed embodiments. Applicants respectfully note that the above argument pointing out that

Ishibashi et al. disclose common signals stored in encrypted form applies equally to Heer (see the abstract, for example).

Turning next to the claims, claim 1 is directed to a semiconductor integrated circuit that is provided as a monolithic circuit for decryption of broadcast signals that include picture and sound components. The circuit is recited as including, *inter alia*, an input interface, a processing unit arranged to receive encrypted broadcast signals from the input interface, a first decryption circuit, and a second decryption circuit in which the only route to placing a common key in the common key store is to input the common key in encrypted form for decryption in accordance with the secret key and provide the common key to the common key store over an internal bus, and further in which the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key.

As discussed above, none of the three references cited and applied by the Examiner provide a common key to a common key store over an internal bus. In other words, this is a hardware implementation to provide additional levels of security. The common keys are not broadcast to the common key store. Rather, they are provided to the common key store over the internal bus.

In view of the foregoing amendments to independent claim 1, applicants respectfully submit that this claim is clearly allowable. Dependent claims 2-9, all of which depend ultimately from claim 1, are allowable for the features recited in these dependent claims as well as for the reasons why claim 1 is allowable.

Independent claim 10 has been amended to include the new features as recited in independent claim 1. These features have also been included in independent claims 13, 16, and 19. Applicants respectfully submit that these independent claims and all claims depending therefrom are allowable for the reasons discussed above with respect to claims 1-9.

In view of the foregoing, applicants respectfully submit that all of the claims in this application are in condition for allowance. In the event the Examiner finds minor informalities that can be resolved by telephone conference, the Examiner is urged to contact the undersigned representative by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

Respectfully submitted,
SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:jl:jms

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031

1185591_1.DOC